Opis systemu zabezpieczeń informatycznych w Centrum Onkologii w Warszawie

1. Opis zabezpieczeń sieci komputerowej

Sieć lokalna jest odseparowana od internetu za pomocą urządzeń klasy UTM (Unified Threat Management – wielofunkcyjne zapory sieciowe). Urządzenie Fortigate 600C posiada następujące kluczowe funkcjonalności:

- antywirus
- IDS/ IPS (Intrusion Detection System / Intrusion Prevention System systemy wykrywania i zapobiegania włamaniom)
- filtr ruchu www
- wykrywanie malware (złośliwe oprogramowanie)
- anty spam.

Urządzenie skanuje cały ruch sieciowy przychodzący i wychodzący stanowiąc pierwszą linie zapewnienia bezpieczeństwa.

Na poziomie komputerów użytkowników jest zainstalowane oprogramowanie antywirusowe oraz uruchomiona zapora sieciowa systemu operacyjnego MS Windows. Te rozwiązania stanowią drugą linie zapewnienia bezpieczeństwa w zakresie ruchu sieciowego (strony www, ftp, komunikatory, transfer plików, itp.)

2. Opis zabezpieczeń poczty e-mail

Strumień danych ruchu poczty e-mail przechodzi przez urządzenie klasy UTM – Fortigate 600C, gdzie w ramach pierwszej linii zapewnienia bezpieczeństwa przesyłane dane polegają kontroli antywirusowe, antyspamowej i wykrywania malware.

Następnie (druga linia zapewnienia bezpieczeństwa) dane pocztowe trafiają do urządzenia bezpieczeństwa FortiMail 100D, gdzie poczta e-mail podlega kontroli antywirusowej, antyspamowej oraz weryfikacji: szarej listy (greylist), reputacji adresu IP nadawcy.

Następnie (trzecia linia zapewnienia bezpieczeństwa) wiadomości pocztowe trafiają docelowo lub przechodzą przez stary serwer poczty e-mail. W ramach tego etapu poczta jest sprawdzana za pomocą oprogramowania antywirusowego ClamAV. Część poczty trafia do skrzynek pocztowych skonfigurowanych na starym serwerze (Linux), a część jest przekazywana na nowy serwer poczty (MS Exchange).

Poczta kierowana na nowy serwer poczty podlega kontroli antywirusowej za pomocą oprogramowania zainstalowanego na tym serwerze.

Czwartą linią zapewnienia bezpieczeństwa jest zainstalowane na komputerach użytkowników oprogramowanie antywirusowe oraz uruchomiona zapora sieciowa systemu operacyjnego MS Windows.

3. Zabezpieczenia serwerów

Na serwerach zastosowana ustawienia konfiguracyjne utrudniające włamanie: zmiana portów standardowych usług dostępu zdalnego np. SSH, zablokowanie możliwości logowanie się poprzez SSL użytkowników na starym serwerze poczty.

4. Zabezpieczenia techniczno – organizacyjne

W Centrum Onkologii w Warszawie do zarządzania uprawnieniami użytkowników w zakresie dostępu do serwerów, uprawnień na sprzęcie komputerowym stosuje się usługę katalogową Active Directory (domena MS Windows).

Dostęp do pomieszczeń Działu Informatyki jest ograniczony za pomocą systemu kontroli dostępu opartego o rozwiązanie elektronicznych kart dostępowych oraz jest objęty monitoringiem wizyjnym. Główna serwerownia jest objęta systemem kontroli dostępu oraz jest objęta monitoringiem wizyjnym.

5. Zabezpieczenia głównego systemu medycznego

Główny system medyczny CGM CliniNet firmy CompuGroup Medical Polska posiada następujące zabezpieczenie techniczne i organizacyjne:

- serwery bazy danych i aplikacyjne są zabezpieczone antywirusowo i funkcjonalnością firewall

- serwery funkcjonuję w formie maszyn wirtualnych (łatwa możliwość uruchomienia nowych z kopii, czy odtworzenia)

- codzienna kopia bezpieczeństwa

- istnienie instancji produkcyjnej i testowej serwerów systemu medycznego. Poprawki i aktualizacja je są najpierw sprawdzane na instancji testowej. Dopiero do pomyślnym wyniku sprawdzenia działania mogą zostać zainstalowana na instancji produkcyjnej.

- informacja o zmianach treści danych jest zapisywana w logu systemu

- indywidualne konta dla każdego z użytkowników oraz poziomy uprawnień dla poszczególnych grup zawodowych

- autoryzacja kwalifikowanym podpisem elektronicznym wyników badań diagnostycznych i opisowych w części jednostek organizacyjnych.

6. Zabezpieczenia głównego systemu administracyjnego

Główny system administracyjny e-Simple firmy Simple S.A. posiada następujące zabezpieczenie techniczne i organizacyjne:

- serwery bazy danych i aplikacyjne są zabezpieczone antywirusowo i funkcjonalnością firewall

- serwery funkcjonuję w formie maszyn wirtualnych (łatwa możliwość uruchomienia nowych z kopii, czy odtworzenia)

- codzienna kopia bezpieczeństwa

- istnienie instancji produkcyjnej i testowej serwerów systemu administracyjnego. Poprawki i aktualizacja je są najpierw sprawdzane na instancji testowej. Dopiero do pomyślnym wyniku sprawdzenia działania mogą zostać zainstalowana na instancji produkcyjnej.

- informacja o zmianach treści danych jest zapisywana w logu systemu.

- indywidualne konta dla każdego z użytkowników oraz poziomy uprawnień dla poszczególnych grup zawodowych.

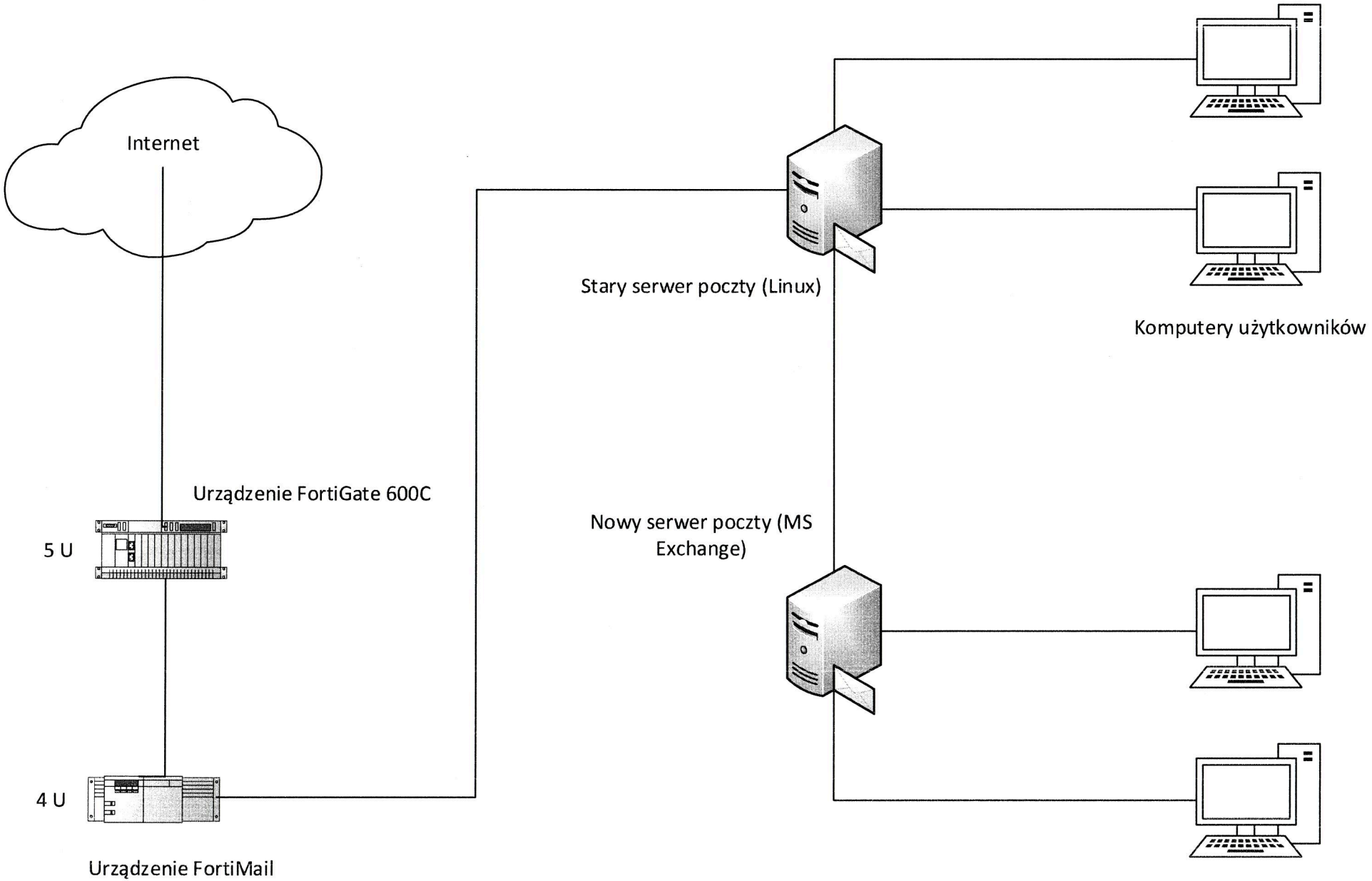
7. Bezpieczeństwo pożarowe głównej serwerowi

W wydzielonym pomieszczeniu głównej serwerowni jest możliwość odcięcia zasilania z poziomu szafek elektrycznych znajdujących się wewnątrz pomieszczenia oraz z poziomu szafy znajdującej się na zewnątrz pomieszczenia.

W pomieszczeniu oraz w jego okolicy znajduje się sprzęt gaśniczy przeznaczony do gaszenia urządzeń elektronicznych.

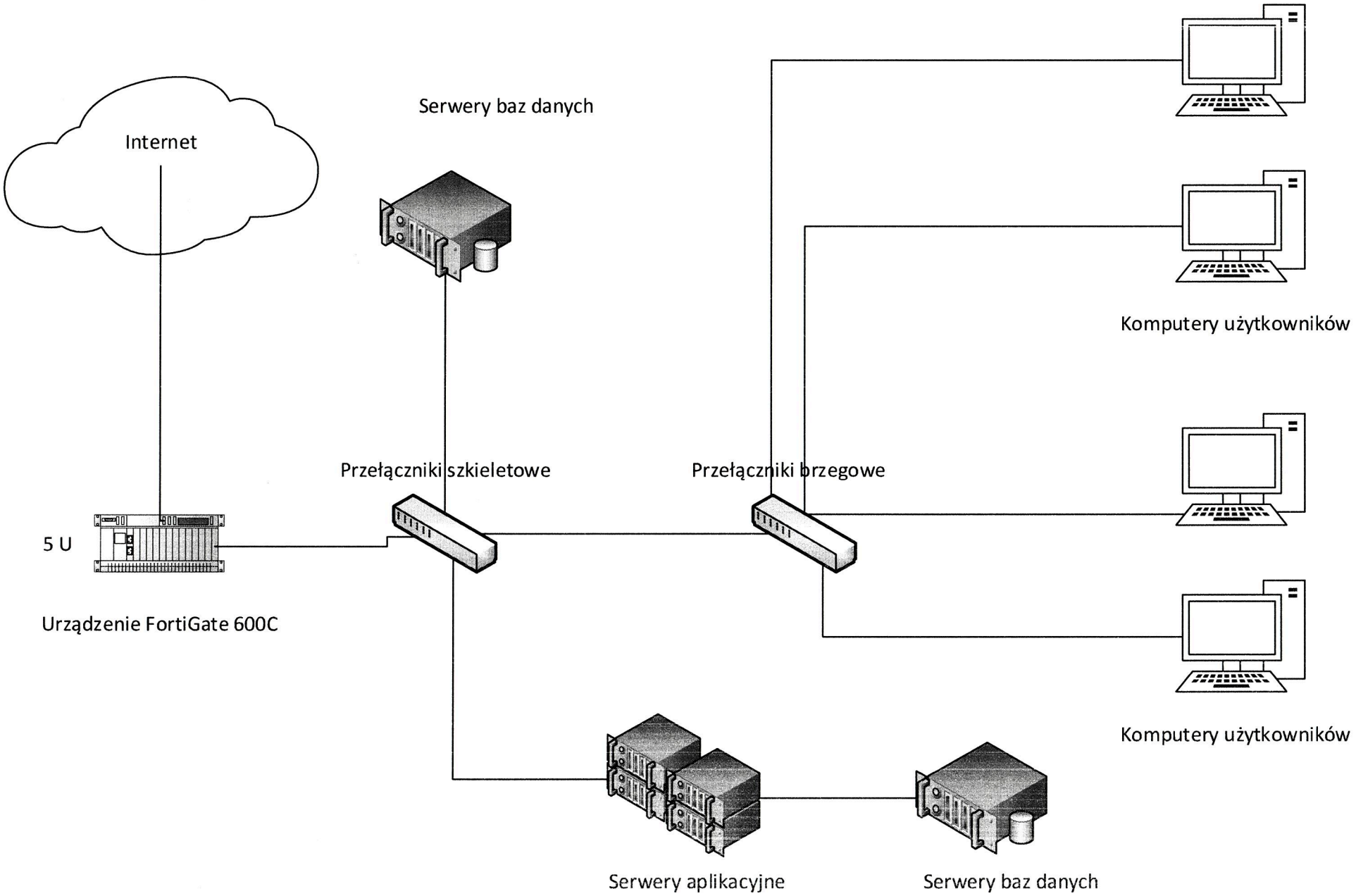
Załączniki:

1. Schemat ruchu sieciowego w COI - plik 20190904_schemat_ruchu_sieciowego_w_COI Warszawa.pdf
2. Schemat ruchu poczty e-mail w COI – plik 20190904_schemat_ruchu_poczty_e-mail_w_COI_Warszawa.pdf



Schemat ruchu poczty e-mail w COI Warszawa

opracował Andrzej Zgódka



Schemat ruchu www sieciowego w COI Warszawa

opracował Andrzej Zgódka